IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	: **10/531,939**
Applicant	: **KAMPERMAN et al.**
Filed	: **4/19/2005**
Confirmation	: **4488**
TC/A.U.	: **2431**
Examiner	: **VAUGHAN, Michael R.**
Atty. Docket	: **NL021063US**

Title: **METHOD AND DEVICE FOR AUTHORIZING CONTENT OPERATIONS**

Mail Stop: **APPEAL BRIEF - PATENTS**
Commissioner for Patents
Alexandria, VA 22313-1450

REPLY BRIEF UNDER 37 CFR 41.41

Sir:

This is a Reply Brief in response to the Examiner's answer dated 5 March 2010 in the subject application.

RESTATEMENT OF GROUNDS OF REJECTION

Claims 1-3, 5-6, 8-10, 12-13, and 31 stand rejected under 35 U.S.C. 102(b) over Jonsson (WO 01/76294).

Claims 4 and 11 stand rejected under 35 U.S.C. 103(a) over Jonsson.

Claims 7 and 21 stand rejected under 35 U.S.C. 103(a) over Jonsson in view of Messerges et al. (USPA 2002/0157002, hereinafter Messerges).

Claims 14 and 32 stand rejected under 35 U.S.C. 103(a) over Jonsson in view of Saw et al. (USP 7,020,781, hereinafter Saw).

Claims 15-17 and 19 stand rejected under 35 U.S.C. 103(a) over Jonsson in view of Wyman (USP 5,204,897).

Claim 18 stands rejected under 35 U.S.C. 103(a) over Jonsson and Wyman in view of Moskowitz et al. (WO 01/18628, hereinafter Moskowitz).

Claim 20 stands rejected under 35 U.S.C. 103(a) over Jonsson in view of Kahn et al. (USP 6,135,646, hereinafter Kahn).

REMARKS REGARDING EXAMINER' ANSWER

Claims 1-21 and 31-32

The applicants believe that the Examiner has misapprehended or overlooked a key element in the applicants' claims; in particular, the Examiner has misapprehended or overlooked the fact that in the applicants' claimed method and device, the users do not expressly grant access rights to each other, per se.

The Examiner refers to one of the users in the applicants' claims as a 'controlling user' and the other as a 'requesting user'; the term 'controlling user' is a misnomer. In the applicants' claims, neither user 'controls' the access of the other user.

For ease of reference, hereinafter the applicants will refer to the claimed 'first user' as the 'first/requesting' user, and the claimed 'second user' as the 'second/authorized' user.

As claimed in claim 1, upon which claims 2-7 and 31 depend, the method includes:

> receiving a user right certificate that identifies a second/authorized user and authorizes the second/authorized user to perform the requested operation on the content item, and
>
> authorizing the operation on the machine by the first/requesting user upon receipt of information from the first/requesting user that links the first/requesting user and the second/authorized user as members of a common authorized domain.

Independent claim 8, upon which claims 9-21 and 32 depend, includes similar features to claim 1.

Of particular note, as claimed in claims 1 and 8, the second/authorized user does not control or authorize the operations by the first/requesting user. The first/requesting user need only provide information that identifies the first/requesting and second/authorized users as members of the same domain.

As the Examiner acknowledges: "Jonsson teaches that the controlling user gives to the requesting user access to his client structure" (Answer, page 13, lines 9-10). This is contrary to the claimed granting of rights based solely on showing that (any) second/authorized user is authorized to perform the operation and receiving information from (any) first/requesting user that links the first/requesting user to the second/authorized user in a common domain.

The Examiner also acknowledges that:

> "Jonsson teaches that each client structure has a superuser (controlling user) which has the entire set of rights for the client structure. Superusers can then assign rights to other users in that particular client structure… Once a supervisor identifies himself as the superuser of his/her domain, the act of assigning another user to said domain can proceed." (Answer, page 13, lines 16-21).

That is, Jonsson specifically requires the superuser/controlling user to take an active part in assigning user rights, which is contrary to the claimed authorizing of operations based solely on a user right associated with an authorized user, and information from a requesting user that links the requesting user to the authorized user.

In mapping the steps of Jonsson to the claimed method, the Examiner first notes that the "machine/server must have access to the controlling user's authority profile for authentication purposes" (Answer, page 14, lines 1-2). Assuming in argument that Jonsson's authority profile can be said to correspond to a user right certificate, the applicants acknowledge that this step may arguably be said to correspond to the first element of claim 1: "receiving, at the machine, a user right certificate that identifies a second [authorized] user and authorizes the second [authorized] user to perform the requested operation on the content item."

However, the Examiner subsequently notes that the "identified controlling client can then create an authority profile of his client structure for the requesting user as evident by the fact that he defines which services the requesting user will have access to" (Answer, page 14, lines 2-5). The applicants agree with this characterization of Jonsson's authorization process, but respectfully maintain that this process cannot reasonably be said to correspond to the second element of claim 1: "authorizing the operation on the machine by the first [requesting] user upon receipt of information from the first [requesting] user that links the first [requesting] user and the second [authorized] user as members of a common authorized domain."

In particular, the authorization process characterized by the Examiner does not require any action on the part of the first/requesting user, while the applicants' claimed invention does not require any action on the part of the second/authorized user. Correspondingly, the authorization characterized by the Examiner requires action on the part of the second/authorized user, while the applicants' claimed invention requires action on the part of the first/requesting user.

The Board has consistently upheld the principle that the burden of establishing a prima facie case resides with the Office, and to meet this burden, the Examiner must specifically identify where each of the claimed elements is found in the prior art:

> "there must be ***no difference*** between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention. Scripps Clinic & Research Found. v. Genentech, Inc., 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991). To meet [the] burden of establishing a prima facie case of anticipation, the examiner must explain how the rejected claims are anticipated by pointing out where all of the

> ***specific limitations*** recited in the rejected claims are found in the prior art relied upon in the rejection." *Ex Parte Naoya Isoda*, Appeal No. 2005-2289, Application 10/064,508 (BPAI Opinion October 2005).

The applicants respectfully maintain that the difference in user roles and the different actions required of the users between Jonsson and the applicants' claimed invention cannot be said to correspond to the disclosure of identical inventions, and that, because of these differences, the Examiner cannot be said to have identified where Jonsson teaches each of the specific limitations recited in the claims.

The applicants believe that the Examiner's ending statement on this issue clearly indicates the Examiner's overlooking of a key element in the applicants' claims, which is that the second/authorized user is not a controlling user, and has no direct control of whether any other member of the domain is granted access:

> "By the reference, the requesting user may perform an operation on content because he/she has been authorized to do so by the controlling user" (Answer, page 15, lines 1-15).

In contrast, in accordance with the applicants' invention: the requesting user may perform an operation on content merely because he is a member of a common domain of an authorized user.

The applicants note that the differences between Jonsson and the applicants' claimed invention has a significant impact on the utility of the authorization process. Jonsson's example applications include granting employees of a company particular access rights, and a homeowner's granting of rights to a neighbor for control of particular appliances while the homeowner is away (Johnson, page 7, second paragraph). Jonsson's main focus is allowing a user to selectively grant rights to other users, and Jonsson's implementation provides this selective granting of rights by an authorized user.

Conversely, the applicants address a more egalitarian environment, such as a family, wherein any member of the family is granted access to any content material that any other member of the family has access to. The applicants disclose that the ability to provide equal access among family members is a desired characteristic that poses a problem to prior art digital rights management (DRM) systems:

> "At present it is possible for one member of a family to purchase (a right to) a content item, for example a song stored on a compact disc, which he can share with the other members of that family. Consumers are used to such sharing and they expect it from AD-based systems as well. Copyright law typically permits such activities as long as they stay within a particular family. DRM systems try to prevent copying to any third party, and so inadvertently also block this permitted type of activity." (Specification, page 2, line 30 – page 3, line 4.).

A primary focus of the applicants' solution is allowing equal access to content material among members of such an egalitarian group:

> "It is desirable to be able to share access to the content item with members of a particular family, or more generally a particular domain. To this end, domain certificates (certificates to indicate a group or domain) are issued by a trusted third party to define which persons are member of a particular domain. If the first user now is not authorized to perform the operation, but there is a second user in the same domain who does have such a right, then the first user is still allowed to perform the operation." (Specification, page 4, lines 2-9.)

The applicants' claimed invention allows these equal rights to any member of the domain by allowing the member to merely provide information linking this member to another member who has been granted the desired rights.

Although it may be argued that the applicants' second/authorized user is a controlling user because this user can withhold the user right certificate, if this second/authorized user withholds the user right certificate, the first element of the claim is not satisfied. In the applicants' claimed invention, the system must receive the second/authorized user's right certificate, at which point the second/authorized user relinquishes any and all control of the other domain members' access rights.

Because the second/authorized user in the applicants' claimed invention has no control over the rights granted to members of the authorized domain, the applicants' claimed invention would be unsuitable for use in Jonsson's user-controlled-rights applications, just as Jonsson's invention would be unsuitable for use in the applicants' equal-rights applications.

Because Jonsson does not teach authorizing an operation by a first/requesting user upon receipt of information from the first/requesting user that links the first/requesting user and a second/authorized user as members of a common authorized domain, as claimed in claims 1 and 8, and because Jonsson specifically teaches a contrary solution to the task of authorizing operations, the applicants respectfully maintain that the rejections of claims 1-21 and 31-32 that rely on Jonsson for teaching the elements of claims 1 and 8 are unfounded, and should be reversed by the Board.

Claims 2-4, 6-7, 9-21 and 32

The applicants respectfully maintain that the Examiner has adopted an overly broad interpretation of the term "domain certificate" that is not consistent with the use of the term in the applicants' specification.

The Examiner asserts that the definition provided in the specification cannot be read into the claims, and therefore the term must be read broadly. The applicants respectfully disagree with this assertion.

The applicants have specifically defined the term 'domain certificate' as a term with specific meaning:

> "In order to introduce the notion of Authorized Domain, we propose to introduce another type of certificate into the system. A certificate, which we call a domain certificate, is issued by a (trusted) third party that defines what persons/entities belong to a certain domain. Such a certificate contains the identifier (e.g. biometric, public key) of the subject (a person) and the identifier (e.g. name, public key) of the authorized domain the subject is declared to be part of. The certificate is signed with the private key of the issuing trusted party. Furthermore the certificate must contain the usual fields like 'date of issue' and 'validation date' in correspondence with an

> appropriate revocation system. The SPKI ‘name certificate’ could be used to implement this domain certificate." (Specification, page 9, lines 15-23.)

It is well established that an applicant can define terms used in the specification, and that such terms will control their interpretation in the claims:

> "Where an explicit definition is provided by the applicant for a term, that definition will control interpretation of the term as it is used in the claim. *Toro Co. v. White Consolidated Industries Inc.*, 199 F.3d 1295, 1301, 53 USPQ2d 1065, 1069 (Fed. Cir. 1999) (meaning of words used in a claim is not construed in a "lexicographic vacuum, but in the context of the specification and drawings"). (MPEP 2111.01 IV: APPLICANT MAY BE OWN LEXICOGRAPHER.)

Accordingly, the applicants respectfully maintain that the interpretation of the term 'domain certificate' in the claims must be consistent with the term as defined within the applicants' specification.

Alternatively, assuming in argument that the term 'domain certificate' should be interpreted using its plain meaning, the applicants respectfully maintain that the Examiner's interpretation of this term as including Jonsson's client structure is inappropriate.

The plain language meaning of the term 'certificate' is a "document testifying to the truth of something" and the plain language meaning the term 'domain' is a "sphere of activity, concern, or function".[1] A plain language meaning of a domain certificate would lead one to conclude that it is likely a document that certifies the extent of some sphere of activity. Recognizing that the field of the art is electronic based, one would likely conclude that this certifying document is in digital form.

The applicants' claim is that this domain certificate is received from the first/requesting user, and identifies the first and second users as members of a common authorized domain. In light of the claim language and the plain meaning of the term 'domain certificate', one would likely conclude that the first/requesting user must somehow communicate this digital certification to the machine.

[1] The American Heritage® Dictionary of the English Language

The Examiner asserts that Jonsson's internal data structure, the 'client structure', corresponds to a 'domain certificate' (Answer, page 4, lines 14-16). The applicants respectfully maintain that this assertion is contrary to both the plain language interpretation of the term 'domain certificate', as well as the definition specifically provided in the applicants' specification. Jonsson's client structure is not a certifying document that is communicated to the machine by a first/requesting user.

Of particular note, Jonsson does not address how one would certify the authorizations defined by the client structures. Inherent in the term 'certificate' is some form of 'certification', and thus applying the term 'certificate' to this internal data structure is not supported in Jonsson.

Jonsson also does not teach that this client structure is received from the first/requesting user. Jonsson specifically teaches that the second/authorized user controls the granting of rights via these client structures; therefore, allowing the first/requesting user to provide these client structures would render Jonsson's invention unsuitable for its intended purpose. In the above mentioned example applications of Jonsson's invention, allowing the first/requesting user to provide the client structure would allow each employee to define which company services the employee has access to, and would allow a neighbor to define which appliances of the homeowner the neighbor can control. Such an interpretation is obviously contrary to Jonsson's teachings.

Because the Examiner's interpretation of the term 'domain certificate' to include Jonsson's internal data structure is inconsistent with both the plain meaning of the term and with the definition specifically provided by the applicants, and because the Examiner's interpretation would render Jonsson's invention unsuitable for its intended purpose, the applicants respectfully maintain that the rejections of claims 2-4, 6-7, 9-21 and 32 that are based on this interpretation are unfounded, and should be reversed by the Board.

CONCLUSIONS

Because Jonsson fails to teach authorizing an operation by a first/requesting user upon receipt of information that links the first/requesting user to a second/authorized user as members of a common authorized domain, the applicants respectfully request that the Examiner's rejection of claims 1-3, 5-6, 8-10, 12-13, and 31 under 35 U.S.C. 102(b) and claims 4, 7, 11, 14-21, and 32 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Because Jonsson does not teach that the information provided by the first/requesting user comprises one or more domain certificates identifying the first and second users as members of the authorized domain, the applicants respectfully request that the rejection of claims 2-3, 6, 9-10, and 12-13 under 35 U.S.C. 102(b) and claims 4, 7, 11, 14-21, and 32 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,

/Robert M. McDermott/
Robert M. McDermott, Esq.
Registration Number 41,508
Phone: 804-493-0707
for: Kevin C. Ecker
Reg. 43,600
914-333-9618

Please direct all correspondence to:
Corporate Counsel
Philips Intellectual Property and Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9618
Fax: (914) 332-0615